

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____

AUG 14 2017

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ DEPUTY

IN THE MATTER OF THE SEARCH OF

INFORMATION ASSOCIATED WITH
THE CELLULAR TELEPHONE
ASSIGNED CALL NUMBERS (202) 807-
8720 AND (202) 870-0270 WITH
INTERNATIONAL MOBILE
SUBSCRIBER IDENTITY /
ELECTRONIC SERIAL NUMBER
355312087899126, THAT IS STORED AT
PREMISES CONTROLLED BY VERIZON
WIRELESS;

INFORMATION ASSOCIATED WITH
THE CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (202) 870-
2419, WITH INTERNATIONAL MOBILE
SUBSCRIBER IDENTITY /
ELECTRONIC SERIAL NUMBER
353817087583795, THAT IS STORED AT
PREMISES CONTROLLED BY T-
MOBILE/METROPCS; AND

INFORMATION ASSOCIATED WITH
THE ACCOUNT FURTHER DESCRIBED
IN ATTACHMENT A-3, THAT IS
STORED AT PREMISES CONTROLLED
BY INSTAGRAM, LLC

18 - 2095 - ADC

18 - 2096 - ADC

18 - 2097 - ADC

Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Sung Kim of the Federal Bureau of Investigation ("FBI"), being
first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application pursuant to Federal Rule of Criminal Procedure 41 for search warrants for (1) information associated with the cellular telephone assigned call numbers (202) 807-8720 and (202) 870-0270 , with International Mobile Subscriber Identity/Electronic Serial Number 355312087899126 that is stored at premises controlled by Verizon Wireless, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921 (**"TARGET TELEPHONE 1"**); (2) information associated with the cellular telephone assigned call number (202) 870-2419, with International Mobile Subscriber Identity/Electronic Serial Number 353817087583795 (**"TARGET TELEPHONE 2"**), that is stored at premises controlled by T-Mobile/MetroPCS, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054; and (3) records and other information in the possession of Instagram LLC pertaining to the Instagram account associated with the username **"freshconscious"** (the **"TARGET ACCOUNT"**).

2. The information to be searched is described in the following paragraphs and in Attachments A-1, A-2, and A-3, respectively. Regarding **TARGET TELEPHONE 1** and **TARGET TELEPHONE 2**, this affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require (1) Verizon Wireless to disclose to the government copies of the information further described in Section I of Attachment B-1; (2) T-Mobile/MetroPCS to disclose to the government copies of the information further described in Section I of Attachment B-2; and (3) Instagram to disclose to the government copies of the information further described in Section I of Attachment B-3 Upon receipt of the information

described in Section I of Attachment B-1, B-2, and B-3, government-authorized persons will review the information to locate items described in Section II of Attachment B-1, B-2, and B-3.

3. I am a Special Agent of the Federal Bureau of Investigation and am currently assigned to a Maryland Joint Violent Crime Task Force comprised of FBI agents, detectives from the Baltimore Police Department (BPD), Baltimore County Police Department (BCDP) and from the Howard County Police Department (HCPD). I have worked for the FBI since 2008 and have participated in numerous investigations focusing on violent crimes, to include bank robberies, Hobbs Act robberies, kidnappings, extortions, and fugitives. I have also participated in the execution of numerous state and federal search and arrest warrants involving violent offenders.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Since this Affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2113 (Bank Robbery); and 18 U.S.C. § 924(c) (Use or Carrying a Firearm in Relation To a Crime of Violence) (the "Target Offenses") are located within **TARGET TELEPHONE 1, TARGET TELEPHONE 2,** and the **TARGET ACCOUNT.**

GENERAL INFORMATION REGARDING INSTAGRAM

it.” He then made motions toward his waist implying he had a weapon. After receiving money from the teller, the suspect fled the bank and entered a red in Dodge Challenger parked in the shopping center’s parking lot.

29. A Howard County Police robbery Detective responded to the scene along with the FBI Special Agents and spoke with the bank employees, reviewed the interior security footage, and learned the following:

- a. The suspect entered the bank branch through the main entrance.
- b. Based on security footage and witness observations the suspect was observed to be at least six feet tall and a heavy build.
- c. He approached the teller counter holding a few \$20 bills.
- d. Once at the counter, the suspect presented a handwritten note to the teller on a yellow sticky type piece of paper.
- e. The note stated, “This is a bank robbery. Don’t do anything stupid. I have a weapon and I will use it”.
- f. The suspect verbally demanded all the \$50 and \$100 bills.
- g. The suspect motioned towards his waist with his hand, making the victim believe that he had a weapon.
- h. The suspect was provided \$600 in United States currency from the teller drawer and subsequently fled the bank.
- i. Another bank employee was notified by the victim of the robbery that a robbery had just occurred.
- j. That employee ran out of the bank and followed the suspect to a nearby parking lot.
- k. The suspect attempted to enter the driver’s door of a parked red Dodge Challenger.

- l. At that time, the suspect observed the bank employee photographing him with his cell phone.
- m. The suspect threatened the bank employee by stating, "I'm going to fuck you up and I'm going to come back and kill both of you all!"
- n. The bank employee then retreated to the bank in fear for his safety.

30. Through additional investigation, security footage was located from the surrounding shopping center; it recorded the suspect's red Dodge Challenger arriving in the shopping center several minutes prior to the robbery. The same vehicle was also recorded leaving the shopping center just after the robbery.

31. Through further investigation and research, Howard County investigators determined the suspect vehicle to be a 2015-2016 factory year Dodge Challenger based upon its body style and design.

32. As part of this ongoing investigation, during March of 2018, investigators conducted database checks utilizing various law enforcement resources, including vehicle collision data involving any and all 2015 red in color Dodge Challenger passenger vehicles. Collision data involving similar vehicles were researched to explore if any involved parties matched the suspect's description.

33. Through those inquiries, the investigators located collision data involving a 2015 red Dodge Challenger, which was dated January 19, 2018. The collision was reported to Washington D.C., Metropolitan Police Department (MPD) and occurred in Washington D.C. The owner/involved party of this collision was identified as Reginald Ricks, a black male, born December 27, 1989. Ricks currently possesses an Indiana state driver's license.

34. Ricks' physical description on the license indicated he was six feet and two inches

tall and that he weighed approximately 253 pounds. The investigators also located a current on file photograph of Ricks through the Indiana Department of Motor Vehicles.

35. Upon viewing that photograph and more recent social media photographs of Ricks, it was determined that Ricks closely matched the suspect in the December 30, 2017 bank robbery by physical description and appearance, including height and approximate build. Additional checks found that although Ricks held and reported an Indiana address for his current Indiana driver's license, the Dodge Challenger's Indiana registration listed a mailing address of 410 Taylor Street, N.E., #23B, Washington, D.C. 20017—Ricks' home.

36. Criminal record checks of Ricks also revealed an incident on December 20, 2012, in which Ricks was a suspect in connection with a PNC Bank robbery in Prince Georges County, MD that was similar in nature to the armed bank robbery in Howard County. As in the December 30, 2017, robbery, the 2012 PNC Bank robbery also involved a bank that was located within a Giant grocery store. Furthermore, the suspect's description from the December 20, 2012, robbery was consistent with the description of Ricks—a tall black male with a large build.

37. On March 20, 2018, the investigators learned of another PNC Bank robbery that occurred in Baltimore City, MD on March 18, 2018 at approximately 1419 hours. In that incident, a large build, medium brown skinned black male described as at least 6'0" tall and approximately 300 pounds entered the bank, approached a teller, and announced a robbery. The suspect displayed a silver revolver that was concealed inside a distinct blue binder with white lettering on the front when he demanded the money. He was not wearing a mask and his face was exposed. As in the December 30, 2017, robbery and the December 20, 2012 robbery, the March 18, 2018 robbery also occurred at a PNC Bank located within a Giant grocery store.

38. During the course of this investigation, investigators accessed a law enforcement

vehicle collision database and learned that Ricks's Dodge Challenger was involved in two separate collisions in the District of Columbia during the month of January 2018. In this collision data, Ricks had reported a phone number of 202-870-0270—one of the numbers associated with **TARGET TELEPHONE 1**—as his point of contact.¹ Investigators also verified that this particular number was serviced by Verizon Wireless.

39. After the investigators reviewed the security footage of the robbery suspect from inside the PNC Bank robbed on March 18, 2018, the investigators would note a significantly close resemblance to Reginald Ricks, the suspect in the PNC Bank robbery on December 30, 2017. The investigators further noted that the facial features, physical stature, size, and skin tone of the two robbery suspects on December 30, 2017 and March 18, 2018 were significantly similar. Finally, as noted above, both incidents occurred within PNC Bank locations inside of Giant grocery stores.

40. On April 11, 2018, United States District Court for the District of Columbia issued a search and seizure warrant for Rick's residence at 410 Taylor Street Apartment 23B, Northeast, Washington, District of Columbia 20017 where he lived with his girlfriend, Courtnie Wilson. On April 12, 2018, a state arrest warrant was issued for Ricks in connection with the robbery that occurred in Howard County.

41. On April 13, 2018, members of the FBI, HCPD and Metropolitan Police Department executed the search and seizure warrant. Ricks and Wilson were in the residence at the time of the execution of the search warrant. During the search of the residence, Ricks'

¹ According to records obtained from Verizon, 202-807-8720, the other phone number associated with **TARGET TELEPHONE 1**, became effective on February 16, 2018, and the effective date of 202-870-0270 was from August 31, 2016 through February 16, 2018.

phone, an iPhone 7, IMEI 355312087899126 (**TARGET TELEPHONE 1**) and Wilson's phone, an iPhone 7 Plus, IMEI 353817087583795 (**TARGET TELEPHONE 2**) were recovered and seized by law enforcement.

42. On April 14, 2018, law enforcement conducted an analysis and review of **TARGET TELEPHONE 1** and **TARGET TELEPHONE 2**. Images of Ricks wearing a camouflage shirt similar to the camouflage shirt worn by the suspect in the Howard County PNC bank robbery were recovered on **TARGET TELEPHONE 1**. Such an image is also visible on Ricks' Instagram account—the Instagram account associated with the user name “freshconscious” (the **TARGET ACCOUNT**)—an account which law enforcement also identified during the search of **TARGET TELEPHONE 1**.² **TARGET TELEPHONE 2** contained, among other things, a text message exchange between Ricks and Wilson concerning the location of Rick's gun and various web searches concerning bank robbery investigations, bank security measures, and the 2012 robbery in Prince Georges County for which Ricks is a suspect. It likewise reflected a search concerning a “howard county robbery.” During an interview with law enforcement, Wilson stated that Ricks used her phone on occasion, but claimed that Ricks only used it to look at social media.

43. On July 24, 2018, a federal grand jury returned an indictment charging Ricks with three counts of Bank Robbery in violation of 18 U.S.C. §§ 2113(a) and one count of Brandishing of a Firearm during a Crime of Violence in violation of 18 U.S.C. § 924(c)(1)(A)(ii).

CONCLUSION

44. I have learned that Verizon Wireless and MetroPCS (the “Providers”) are

² Law enforcement observed the images of Ricks wearing the camouflage shirt on the publicly available version of Ricks' Instagram account.

companies that provide cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

45. Based on my training and experience, I know that Verizon Wireless can collect cell-site data about the **TARGET TELEPHONE 1** and that MetroPCS can collect cell-site data about the **TARGET TELEPHONE 2**. I also know that the Providers typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

46. Based on my training and experience, I know that the Providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that the Providers typically collect and retain information about their subscribers’ use of the wireless service, such as records about

calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify **TARGET TELEPHONE 1** and **TARGET TELEPHONE 2**'s user or users and may assist in the identification of co-conspirators. It likewise can be used to identify the past movements of the users of **TARGET TELEPHONE 1** and **TARGET TELEPHONE 2** within broad (multi-square-mile) geographic regions to determine whether they were present in the areas of other bank robberies during 2017 and early 2018 that shared a similar *modus operandi* to those of the bank robberies discussed above.

AUTHORIZATION REQUEST

47. Based on the foregoing, I request that the Court issue the proposed search warrants, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

48. I further request that the Court direct Verizon Wireless, T-Mobile MetroPCS, and Instagram to disclose to the government any information described in Section I of Attachments B-1, B-2, and B-3, respectively, that is within their possession, custody, or control.

49. Because the warrants will be served on Verizon Wireless, T-Mobile MetroPCS, and Instagram who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

[INTENTIONALLY LEFT BLANK]

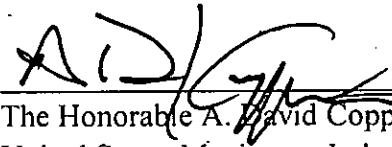
The United States also requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this application and Order.

Respectfully submitted,



Sung Kim
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this 30th day of July 2018.



The Honorable A. David Copperthite
United States Magistrate Judge

ATTACHMENT A1
Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number (202) 807-8720 and (202) 870-0270, with International Mobile Subscriber Identity/Electronic Serial Number 355312087899126 ("the Account"), that are stored at premises controlled by Verizon Wireless ("the Provider"), headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921.

ATTACHMENT B1
Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A1 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A1 for the time period January 1, 2017 to April 14, 2018:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell towers and sectors through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of (1) 18 U.S.C. § 2113 (Bank Robbery); and (2) 18 U.S.C. § 924(c) (Use or Carrying or Brandishing a Firearm in Relation To a Crime of Violence).

ATTACHMENT A2
Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number (202) 870-2419, with International Mobile Subscriber Identity/Electronic Serial Number 353817087583795 ("the Account"), that are stored at premises controlled by T-Mobile/MetroPCS ("the Provider"), headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.

ATTACHMENT B2
Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A2 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A2 for the time period January 1, 2017 to April 14, 2018:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell towers and sectors through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of (1) 18 U.S.C. § 2113 (Bank Robbery); and (2) 18 U.S.C. § 924(c) (Use or Carrying or Brandishing a Firearm in Relation To a Crime of Violence).

ATTACHMENT A3—INSTAGRAM

Property to Be Searched

This warrant applies to information and records that are stored at premises owned, maintained, controlled, or operated by Instagram, LLC a social-networking company headquartered at 1601 Willow Road, Menlo Park, California, 94025, pertaining to the following Instagram account (the “SUBJECT ACCOUNT”):

- The Instagram account associated with the username **freshconscious**

ATTACHMENT B3—INSTAGRAM

I. Files and Accounts To Be Produced By Instagram From January 1, 2012 to Present

To the extent that the information described in Attachment A3 is within the possession, custody, or control of Instagram including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Instagram or have been preserved pursuant to preservation requests made under 18 U.S.C. § 2703(f), Instagram is required to disclose the following information to the government for each account or identifier listed in Attachment A3:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. All information automatically recorded by Instagram from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Instagram website, all information searched for on the Instagram website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;

c. The types of services utilized by the user;

d. All files and records or other information stored by an individual using the account, including all images, videos, documents, communications and other files uploaded, downloaded or accessed using the Instagram service, including all available metadata concerning these files;

e. All records pertaining to communications between Instagram and any person regarding the account, including contacts with support services and records of actions taken;

f. All data and information associated with the personal page and/or profile page, including photographs, videos, audio files, lists of personal interests and preferences, including hashtags;

g. A complete list of all users who are followed by the accounts listed in Attachment A3, and a list of all users who are following the accounts listed in Attachment A3, including every user name, user identification number, corresponding email address, physical address, and date the user joined Instagram;

h. All photos, videos, messages and other files to which the accounts in Attachment A3 have been added, tagged, or associated, including any hashtags or captions associated with each photo, a list of all user who "liked" each photo, a list of each user who commented on each photo, and the substance of each comment regarding each photo.

II. Information To Be Seized By The Government

Any and all records that relate in any way to the SUBJECT ACCOUNT described in Attachment A3 which is evidence, fruits, and instrumentalities of violations of or specifically that relate to 18 U.S.C. § 2113 (Bank Robbery) and 18 U.S.C. § 924(c) (Use or Carrying a Firearm in Relation To a Crime of Violence), as well as:

- a. All records or other information concerning:
 - i. Robbery of any type;
 - ii. All associates of Ricks;
 - iii. Any act of violence;
 - iv. Weapons or items that appear to be weapons; and
 - v. Currency or items that appear to be currency.
- b. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of the above-referenced crimes;
- c. Communication, information, documentation and records relating to who created, used, or communicated with the SUBJECT ACCOUNT, including records about their identities and whereabouts;
- d. Evidence of the times the SUBJECT ACCOUNT listed in Attachment A3 were used;
- e. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- f. Passwords and encryption keys, and other access information that may be necessary to access the SUBJECT ACCOUNT and other associated accounts; and
- g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the SUBJECT ACCOUNT.